ACEEE Int. J. on Network Security , Vol. 5, No. 1, January 2014

Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack

Damandeep Kaur[1] and Parminder Singh[2]
[1] Chandigarh Engineering College Landran, I.T. Department, Mohali, India
Email: sweet.kimi30@gmail.com
[2] Chandigarh Engineering College Landran, I.T. Department, Mohali, India
Email: singh.parminder06@gmail.com

Abstract: Wireless sensor networks are networks having non wired infrastructure and dynamic topology. In OSI model each layer is prone to various attacks, which halts the performance of a network .In this paper several attacks on four layers of OSI model are discussed and security mechanism is described to prevent attack in network layer i.e wormhole attack. In Wormhole attack two or more malicious nodes makes a covert channel which attracts the traffic towards itself by depicting a low latency link and then start dropping and replaying packets in the multi-path route. This paper proposes promiscuous mode method to detect and isolate the malicious node during wormhole attack by using Ad-hoc on demand distance vector routing protocol (AODV) with omnidirectional antenna. The methodology implemented notifies that the nodes which are not participating in multi-path routing generates an alarm message during delay and then detects and isolate the malicious node from network. We also notice that not only the same kind of attacks but also the same kind of countermeasures can appear in multiple layer. For example, misbehavior detection techniques can be applied to almost all the layers we discussed.

Index terms: Wireless Sensor Networks, Promiscuous mode, Wormhole Attack , Malevolent nodes, OSI layers, Attacks.

I. Introduction

WSN are networks which are comprised of large number of sensor nodes deployed over large area that together monitor various environments .WSN's have some unique characteristics that distinguishes it from other wired networks .WSN's have properties like dynamic topology i.e , no particular infrastructure in needed to design an environment and can consist of large number of sensor nodes which can be operated in any environment .Wireless sensor networks are usually centralised means information is gathered at base station or can be collected at aggregation of sensitive nodes. Because of its vulnerable nature, security is one of its major aspect that deserves great attention. This paper classifies the various attacks in OSI layer architecture and their affects are discussed and a security mechanism is proposed to prevent the network layer attack called wormhole attack is prevented by using promiscuous mode methodology.

II. Literature Survey

In [1] author describes the concept of WSN's. Which is comprised of large number of sensor nodes that collaboratively monitor various environments.[2] presented the wormhole attacks and proposed a countermeasure using directional antennas. Co-operative protocol was presented requiring no location information or clock synchronization.[2]defines detection probability model to compute level of transmitter being detected by detection system at arbitrary location around transmitter.[3] analysed that directional antennas provide better capacity gain than that of omnidirectional antenna . Hybrid antenna concept was introduced. [4] describes issues of information protection, analysed them to make methodologies to ensure integrity , authentication and confidentiality.[5]depicted that the threats on adhoc networks faces and security goals to be achieved are studied. Advantage of inherent redundancy in adhoc networks multiple routes between nodes to defend routing against DoS attacks. replication, new cryptographic schemes are cores in secure ad hoc networks.[6] Introduced 3 new mechanisms for key establishments based on framework of pre-distributing a random set of keys to each node.[7] introduced two key distribution schemes random subset assignment key and hypercube based key distribution.[8]Introduced peer intermediaries for key establishment, A class of key-establishment protocols involve using one or more sensor nodes as trusted intermediary.[9] Describes new key distribution scheme which improve resilience of network schemes compared to previous schemes and give in depth analysis.[10] presented symmetric key generation system .Dependencies between keys will exist. Main objective is to decrease uncertainty about keys.[11]Focused on protocols of popular MAC protocol in telling what patterns are observed when an attacker can cause DoS.[12]Designed and studied DoS attack in order to access the damage that is difficult to detect which attackers can cause.[13]Identifies the DoS vulnerabilities author analyzed two different sensor network protocols.[14] Suggested Security based mechanisms on collaborative monitoring technique that prevent active and passive DoS attacks.[15] Described Detection Algorithm to deal with the problem of colluding selfish nodes.[16]Established a classification of

DOI: 01.IJNS.5.1.11

different types of Sybil attack, enabled to better understand the threats posed by each type, proposed several novel techniques. [17] Described new intrusion detection response mechanism that are developed for wireless adhoc network.[18]Examined contention type protocols in non-cooperative environment, where number of stations self optimize their strategies to obtain a more than fair bandwidth share.[19]Implied that with higher programmability of network adapters, the temptation to tamper with the software is likely to grow, can avail larger bandwidth. This paper described two approaches that improves performance of ad hoc network in wormhole attack. In this paper promiscuous mode has been proposed to detect the node which is malicious and then isolating it from the network when all the sensor nodes enters into promiscuous mode. The rest of the paper is organized as follows: Section 3 explains different types of OSI layer attacks in WSNs, Section 4 explains the wormhole attack when two or more colluding nodes makes a tunnel and attract traffic towards it, Section 5 detects and isolate the malicious nodes from the network and enhance performance. Section 6 discusses numerical simulation and results obtained. At the last, Section 7 presents discussion and section 8 presents conclusions and make a projection on possible future research path.

II. OSI Layer Attacks

Among the designs of WSNs, security is one of the most important aspects that deserve great attention, considering the tremendous application opportunities. This chapter will lead readers into this area by presenting a survey of various potential attacks and solutions in WSNs. To ease the presentation, attacks are classified based on the layering model of Open System Interconnection (OSI) (actually only four layers are used).The mechanisms and effects of the attacks in four layers (physical, MAC, network and application), along with potential countermeasures for preventing wormhole attack in network layer.

Table I. OSI Layer Attacks

OSI Layers	Attacks
Application Layer	Clock Skewing, Selective Message Forwarding, Data Aggregation Distortion
Network Layer	False Routing, Packet Replication , Blackhole , Wormhole, Sinkhole
MAC Layer	Traffic Manipulation ,Identity Spook
Physical layer	Device Tampering , Eavesdropping , Jamming

A. Physical Layer

Physical layer in concerned with transmitting raw bites of information over wired or wireless medium [4]. It is responsible for signal detection, modulation, encoding, frequency selection and hence is the basis of network operations [3].

Attacks in Physical Layer: Many attacks target this layer as all upper layer functionalities relies on it. [2] Adversaries do "non technical" things, such as destroying sensors or conduct: technical" actions like wire trapping. Three types of attacks are categorized as:

Eavesdropping: Without sender's and receiver's awareness, eavesdropping attackers can collect the sensitive information and can monitor the data. During transmission, wireless signals are broadcasted in air and are accessible to public. With modest equipment, attacker can easily plug themselves into wireless channel and obtain data. Due to its passive behavior ,it is rarely traceable.

Device Tampering: The simplest way to attack is by damaging the sensors physically and thus stopping the services. Attack will be more threatening if the base station or aggregation points are attacked instead of normal sensor sensors. Since former carries major responsibilities. Another way to attack is to capture sensors and extract sensitive data from them as like spoofing, DoS such attacks are more severe.

Jamming: This attack disrupts the availability of transmission media. This attack introduce intense interference to occupy channels and stops normal sensors to communicate with a device jamming its surrounding sensors, adversaries can disrupt an entire sensor network. In this attack risk of being identified is high, because sensors close to the jamming device can detect higher background contention.

B. MAC Layer

In wireless MAC protocols, typically nodes exchange control packets (CTS and RTS in IEEE 802.11) to gain the right for transmission over the channel for certain period of time [11,15]. Node identifications are embedded in packets to indicate senders and receivers [12,13,14].

Attacks in MAC Layer

Identity Spook: Being of broadcast nature in MAC, identity is visible to all neighbors, including attackers. Without proper protection an attacker can fake an identity and pretend to be different. One example of identity spooking is Sybil attack .An attacker can spoof normal sensor, base station or even aggregation point can cause serious base of further cross layer attacks

Traffic Manipulation: Wireless communication can be easily manipulated in MAC layer. Attackers transmits packet when legitimate users are busy to find out the cause of excessive packet collision, artificially increases contention, decrease signal quality and network availability and hence reduce throughput. this attack breaks the operation of protocols and results in unfair bandwidth usage and thus the performance is degraded in this type of attack

C. Network Layer

Network layer is responsible for locating destinations and calculating optimal path to destination, by tampering with routing services such as modifying routing information and replicating data packets. Attackers can fail communication in WSNs [17].

Attacks in Network Layer: Adversaries can gain access to routing paths and redirects the traffic an can distribute false information among the routing nodes resulting in mislead of routing direction or can launch DoS attack against routing.

DOI: 01.IJNS.5.1.11

False Routing: These are the attacks launched by enforcing false routing information. False routing is of three types:

- False routing attack can be used to place adversary in its desired route.
- It can be used to divert the traffic from one part of network to another.
- It can be used to restrain traffic on certain paths or to bring down a part or entire network.

Blackhole: In this attack the attacker swallows (i.e. receive messages but not forwards) all the messages .By refusing to forward any packet, the attacker affect all the traffic flowing through it. Hence, throughput of all the nodes especially near the attacker are dramatically decreased.

Sinkhole: More complex attack than blackhole attack. Done by getting certain knowledge of routing protocol in use, the attacker tries to attract from particular region through it[16]. Attacker announces a false optimal path by advertising attractive power , bandwidth or high quality routes. Other nodes consider that path better than current path and move their traffic onto it.

Packet Replication: In this attack, Attacker resend packets previously received from other nodes. The packets are then broadcasted to entire network or to particular set of nodes. With large amount of packets replayed, both the bandwidth of network and power of nodes are consumed in vain, leads to the early termination of network operations.

Selective Forwarding: In this type of attack sensor selective forwarding is done by attackers .Attacker senses, discards information from selected sensors. Attack occur when attacker is on the path of multihop networks. Attacker can just discards packet from some selected nodes at its will.

Wormhole attack: In the wormhole attacks, a malevolent node excavates the messages it receives at one end of the network over a separate low-latency channel .Then it repeats messages at a different point in the sensor network. For example, when a source node is passing on data to a destination node then there can be a malicious node in between them which selectively forwards the data packets. The wormhole attacks usually engage two different and far-away malevolent nodes conspire to minimize their remoteness from each other by replaying packets next to an out-of-reach channel which is only available to the attacker

D. Application Layer

This layer implements the services seen by users. For e.g. important application in WSN are data aggregation and time synchronization. Data aggregation sends data collected by sensors to base station and time synchronization synchronizes sensor clocks for co-operative operations [20].

Application Layer Attacks: Attacks in this layer have the knowledge of data semantics, and thus can manipulate the data to change the semantics. As the result, false data are presented to applications and lead to abnormal actions. In this section, the following attacks will be discussed:

Selective Message Forwarding: In this attack adversary is on the path between source and destination and is thus responsible for forwarding packet from source. In this attack adversary need to send the semantic of payload of application layer by treating each packet as meaningful message and select packets to be forwarded based on semantics [20].

Data aggregation distortion: Once data is collected sensors usually send it back to base station for processing. Attacker may maliciously modify the data to be aggregated and make final aggregation and makes final aggregation results computed by base station to be distorted. As a result of which the base station will have incorrect view of environment monitored by sensors.

Clock Skewing: This attack takes place by emitting false timing information. This attacks aims to desynchronize the sensors i.e. skewing the clocks .Once modes adjust their clock based on memory information they will be out of synchronization with access point.

IV. Wormhole Attack

In this section the wormhole attacks modes are explained and classes while pointing to the impact of the wormhole attack. There are various severity attacks in WSN. Wormhole attack is considered as the most dangerous attack in wireless sensor network [20]. It is a dangerous attack because it is independent of MAC layer protocols and are immune to cryptographic techniques. In wormhole attack an attacker creates a link between the true node and the malevolent node, with which the malevolent node attracts the traffic towards it by a very high quality connection which is actually not the high quality connection but just an illusion [27]. The colluder node then creates a covert channel with one or more nodes and then the malevolent node passes message to the another node through covert channel and the other node replay the packets in the network or start dropping selected packets.. Here in Fig.1 X & Y be two Wormhole (Intruder) connected by Wormhole link. X replays in its neighborhood (in area A) everything that Y hears in its own neighborhood (area B) and vice versa. The net effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbors and vice versa. This, as a result, affects routing and other connectivity based protocols in the network. Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption. They can also spy on the packets going through them and use the large amount of collected information to break any network security.

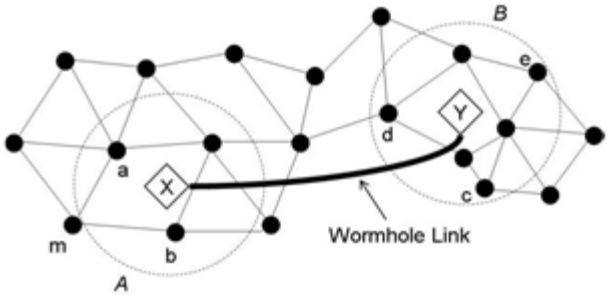

Fig.1 Wormhole Attack

DOI: 01.IJNS.5.1.11

Wormhole Attack Modes: Wormhole attacks can be launched using several modes, among these modes [3], i.e., mentioned as follows:

(1) Wormhole using Encapsulation: In this mode a malicious node at one part of the network and hears the RREQ packet. It tunnels it to a second colluding party at a distant location near the destination. The second party then rebroadcasts the RREQ. The neighbors of the second colluding party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multihop paths. The result is that the routes between the source and the destination go through the two colluding nodes that will be said to have formed a wormhole between them. This prevents nodes from discovering legitimate paths that are more than two hops away. Any routing protocol that uses the metric of shortest path to choose the best route is vulnerable to this mode of wormhole attack. This mode of the wormhole attack is easy to launch since the two ends of the wormhole do not need to have any cryptographic information, nor do they need any special capabilities, such as a high speed wire line link or a high power source.

(2) Wormhole using Out-of-Band Channel: The second mode for this attack is the use of an out of band channel. This channel can be achieved, for example, by using a long range directional wireless link or a direct wired link. This mode of attack is more difficult to launch than the previous one since it needs specialized hardware capability.

(3) Wormhole with High Power Transmission: Another method is the use of high power transmission. In this mode, when a single malicious node gets a RREQ, it broadcasts the request at a high power level, a capability which is not available to other nodes in the network. Any node that hears the high power broadcast rebroadcasts it towards the destination. By method, the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of a colluding node.

(4) Wormhole using Packet Relay: Wormhole using Packet Relay is another mode of the wormhole attack in which a malicious node relays packets between two distant nodes to convince them that they are neighbors. It can be launched by even one malicious node. Cooperation by a greater number of malicious nodes serves to expand the neighbor list of a victim node to several hops. It is carried out by an intruder node X located within transmission range of legitimate nodes A and B, where A and B are not themselves within transmission range of each other. Intruder node X merely tunnels control traffic between A and B (and vice versa), without the modification presumed by the routing protocol.

Wormhole using Protocol Deviations: A wormhole attack can also be done through protocol deviations. During the RREQ forwarding, the nodes typically back off for a random amount of time before forwarding reduce MAC layer collisions. A malicious node can create a wormhole by simply not complying with the protocol and broadcasting without backing off. The purpose is to let the request packet it forwards arrive first at the destination. The utility of organizing combinations of network attacks as graphs is well established. Network attack graphs represent a collection of possible penetration scenarios in a computer network. The graph can focus on the extent to which an adversary can penetrate a network to achieve a particular goal, given an initial set of capabilities. They represent not only specific attacks but categories of attacks. They can detect previously unseen attacks which have common features with attacks in graphs.

V. Promiscuous Mode

To mitigate the WSN from wormhole attack, it has been proposed the method of categorizing nodes based upon their dynamically measured behavior, named as Promiscuous mode [10]. In this paper two extensions to Ad Hoc on Demand Routing protocol (AODV) are implemented in order to mitigate the effect of routing misbehavior during wormhole attack. The two extensions namely Watchdog and Path rater are implemented. Watchdog identifies misbehaving nodes and path rater helps routing protocol (AODV) to avoid these nodes [19]. When node forward packet, the nodes watchdog verifies that the next node in the path also forward the packet. Watchdog does this by listening promiscuously to next nodes transmissions. If next node does not forwards the packet, then it is misbehaving node. Path rater use this knowledge of misbehaving nodes to choose the network path that is most reliable to deliver packets. In this paper during simulations the multihop route is established between the source and destination by the source node then the delay parameters are observed when the delay proceeds from the implied time then the watchdog became active and generate the promiscuous mode. In which all other sensor nodes except the path nodes enters into the promiscuous mode after getting alarm message from source node. The watchdog then detects the malicious node and isolate it from the network and path rater then finds the other most reliable and suitable route to forward the packets from source to destination.

VI. Simulation Results

In this section, results of simulation of AODV with wormhole attack in WSN are shown. The simulations are done in NS2 simulator (version 2.35). In this simulation results on throughput and delay are defined. Parameters used in simulations are summarized as follows

(1) Queue length = 50
(2) Routing protocol=AODV
(3) Packet Size = 1000 bytes
(4) Traffic generator= CBR
(5) Antenna = Omnidirectional
(6) Propagation Ground = 2-way ground
(7) X = 800
(8) Y = 800
(9) Number of nodes = 20
802.11 standard wireless channel

From the Fig.2 It is shown that the throughput before implementing promiscuous mode was very low during wormhole attack and after the methodology implementation the throughput became very high even in the presence of wormhole at

DOI: 01.IJNS.5.1.11

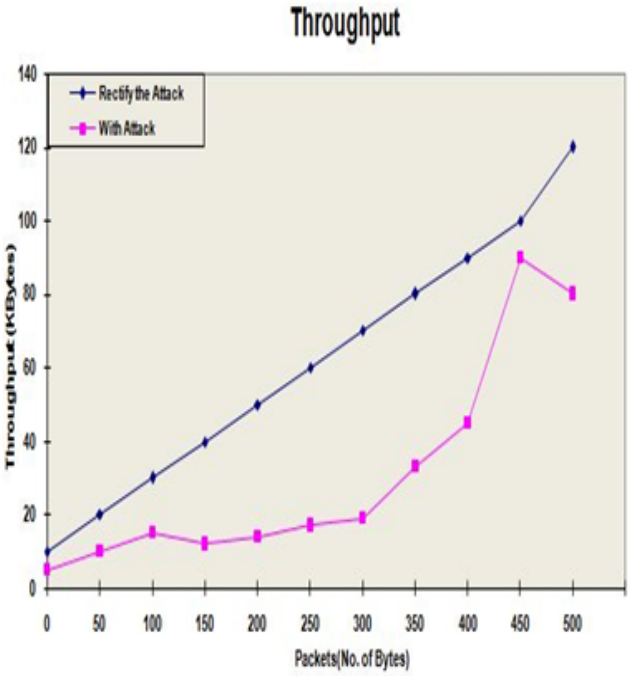

Fig.2 New throughput vs. Old Throughput

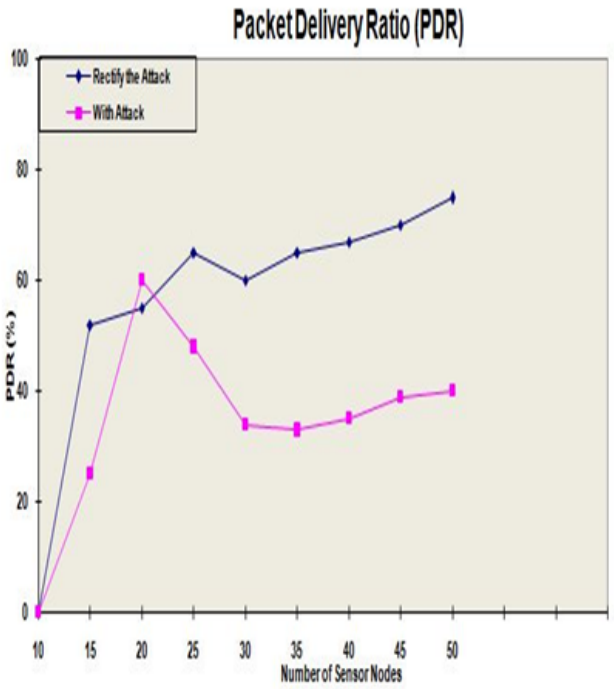

Fig.4 Old PDR vs. New PDR

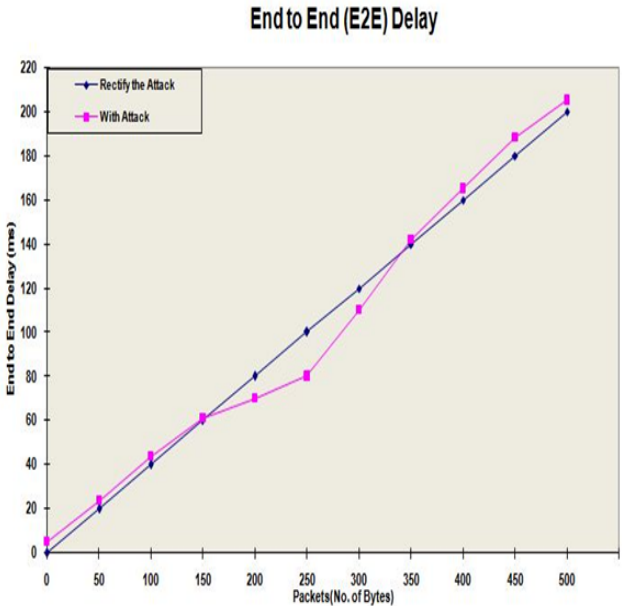

Fig.3 Old delay vs. New delay graph

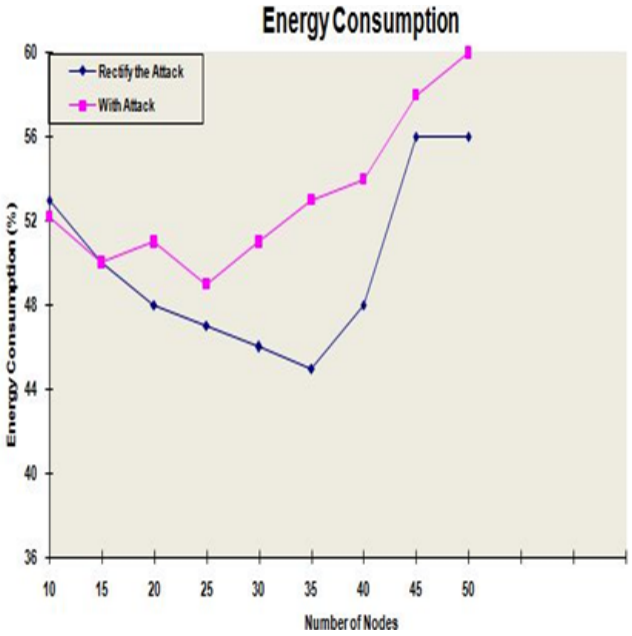

Fig.5 Old Energy vs. New Energy

tack. Fig.3 represents the effect of delay on wireless sensor network during wormhole attack before and after implementing promiscuous mode. There is sharp rise in delay when wormhole attack was done before promiscuous mode implementation. Fig.4 shows the Packet Delivery Ratio (PDR) before and after the implementation of methodology. PDR increases when promiscuous mode in implemented. Fig. 5 shows the old Energy consumed during wormhole attack and New Energy Consumption after the promiscuous mode implemented. The energy consumption decreases when promiscuous mode is implemented. Which shows that methodology been implemented by us works well to isolate malicious node from the network and increases performance metrics as well.

VII. Discussion

Various attacks are discussed in this paper. The attacks in fact are often launched in combination. Combinations can be cross layer in which multiple attacks are launched to lure the sensor nodes which result in sinkhole attack. Such combinations complicate the situation of WSN security and demand further research on countermeasures.

DOI: 01.IJNS.5.1.11

VIII. Conclusion And Future Scope

In this paper promiscuous mode methodology is implemented which works very efficiently in WSNs during wormhole attack. It not only prevents the degradation of the wireless network also helps in improving performance of wireless sensor networks. This methodology has not been proposed yet based on delay metrics. Analysis has been done through simulation to enhance performance of the proposed model in wireless multihop network. The simulation results have shown that in the presence of malicious nodes in ad hoc network. The performance of wireless network with AODV provided extensions with promiscuous mode mechanism is better than wireless network with simple AODV routing protocol in terms of throughput and end to end delay. Furthermore, it can help in putting some constraints on the network topology to design a robust network for such attacks, and in the design of new and more powerful attack countermeasures. In future more complex attacks can be simulated and comparison of their performances can be done to select the optimum method for prevention of attack from attacker's point of view. Once selected, it will be tested with some of the proposed countermeasures and will help in the development of new attack prevention and detection schemes.

References

[1] S. L. Malfa, "Wireless sensor networks," 2010.

[2] L.Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," Network and Distributed System Security Symposium(NDSS), 2004.

[3] M. Takai, J. Martin, R. Bagrodia, and A. Ren, "Directional virtual carrier sensing for directional antennas in mobile ad hoc networks," in MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. New York, NY, USA: ACM Press, 2002, pp. 183–193.

[4] R. Ramanathan, "On the performance of ad hoc networks with beamforming antennas," in MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing. New York, NY, USA: ACM Press, 2001, pp. 95–105.

[5] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, 2003, p. 197.

[6] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in CCS '03: Proceedings of the 10th ACM conference on Computer and communications security. New York, NY, USA: ACM Press, 2003, pp. 52–61.

[7] H. Chan and A. Perrig, "Pike: Peer intermediaries for key establishment in sensor networks," in IEEE Infocom, 2005.

[8] M. Azer, S. El-Kassas, and M. El-Soudani, "A full image of the wormhole attacks-towards introducing complex wormhole attacks in wireless ad hoc networks," 2009.

[9] S. Marti, T. J. Giuli, K. Lai, M. Baker et al., "Mitigating routing misbehavior in mobile ad hoc networks," in International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking, vol. 6, no. 11, 2000, pp. 255–265.

[10] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the mac layer in wireless ad hoc networks."

[11] I. A. Jean-Pierre, "Denial of service resilience in ad hoc networks." 2004.

[12] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54–62, 2002.

[13] P. Michiardi and R. Molva, "Prevention of denial of service attacks and selfishness in mobile ad hoc networks," in Institut Eurecom Research Report RR-02-063, 2002.

[14] A. A. Cardenas, S. Radosavac, and J. S. Baras, "Detection and prevention of mac layer misbehavior in ad hoc networks," in Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks, 2004.

[15] J. R. Douceur, "The sybil attack," in IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems. Springer-Verlag, 2002, pp. 251–260.

[16] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks," Wired Network, vol. 8, no. 5, pp. 521 534,2002.

[17] J. Konorski, "Multiple access in ad-hoc wireless lans with noncooperative stations." in NETWORKING, pp. 1141–1146, 2002

[18] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On cheating in CSMA/CA Ad hoc networks," in EPFL Technical Report, 2004.

[19] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in WMCSA '99: Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications. IEEE Computer Society, 1999, p. 90.

[20] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, no. 2–3, pp. 293– 315, September 2003.

DOI: 01.IJNS.5.1.11